United States Air Force
Date: 14 Dec 96

INFORMATION WARFARE:
NEW ROLES FOR INFORMATION SYSTEMS IN MILITARY OPERATIONS

by Captain George A. Crawford

"... For to win one hundred victories in one hundred battles is not the acme of skill. To subdue an enemy without fighting is the acme of skill."[1]

- Sun Tzu

Introduction

In the past decade we have witnessed phenomenal growth in the capabilities of information management systems. National security implications of these capabilities are only now beginning to be understood by national leadership. Information warfare (IW) is one of the new concepts receiving a great deal of attention inside the Washington DC beltway; in some circles IW is even touted as the cornerstone of future US military doctrine. There is no doubt IW is a concept the modern military officer should be familiar with, for advancements in computer technology have significant potential to dramatically change the face of military command and control.

Information warfare theory has tremendous political, technical, operational and legal implications for the military. This article seeks to define IW for the layman and discuss its potential applications. It will also attempt to identify potential military uses of existing information systems technology and address some of the issues facing those who will be responsible for implementing this new doctrine.

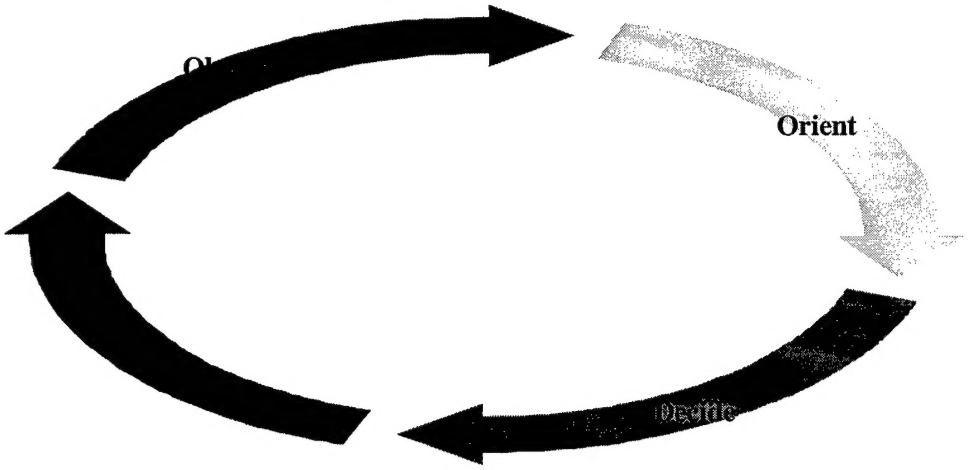
Information Warfare--What is it?

Since the dawn of life, animals have developed senses in order to tell the difference between that which should be eaten and that which might eat them. Governments spend untold billions of dollars establishing agencies to gather and maintain information on potential threats to their security. Computer hackers--most notably members of "The Legion of Doom"[2]--have been tried, convicted and sent to prison because they conspired to provide access to proprietary information. These and countless other examples from current events illustrate a simple premise: information is a strategic asset. We can assess a real dollar value based on potential gain or loss due to the availability of the right information at the right time. The absence of critical information can spell the difference between success or failure in the modern political or military arena. Therefore, the capability to provide or deny critical information may be considered the pinnacle of military or strategic power.

Information warfare, simply put, is an orchestrated effort to achieve victory by subverting or neutralizing an enemy command and control (C^2) system, while protecting use of C^2 systems to coordinate the actions of friendly forces. A successful IW campaign seizes initiative from an enemy commander; the IW campaign allows allied forces to operate at a much higher tempo than an enemy can react to.

The concept of an "OODA Loop" is often used to illustrate information warfare.[3] OODA stands for the steps in a commander's decision making cycle--Observe, Orient, Decide and Act. These steps form the cycle illustrated in Figure 1.

Figure 1. The OODA Loop



A commander **observes** the battlefield situation through all the assets at his disposal. He **orients** his force to take advantage of opportunities and vulnerabilities identified during the observation step. When the force is oriented, the commander **decides** which course of action to take. The commander **acts** by issuing orders, and the force implements his decision. Once the action is in process, the cycle begins again as the commander observes the opposing force's reaction to his moves. The length of time needed for this cycle to complete itself can be illustrated by the OODA Loop's size. This size will be affected by many factors; e.g., the length of time required to collect, analyze and disseminate observations, the amount of time needed to orient forces, the decisiveness of the command structure and the time necessary to communicate a decision to the forces.

At the same time the allied commander is engaged in this process, the opposing command structure is engaged in its own "OODA Loop". Thus, an engagement between two opposing sides can be seen as a competition to possess the smallest OODA loop. The side with the smallest

OODA loop operates at a much higher tempo, forcing the opposing side to react to its moves. Through a successful campaign of subversion, deception and psychological operations, friendly forces can increase the size of an opponent's OODA loop, while reducing the size of their own. If the information warfare campaign is fully implemented, the enemy may ultimately be compelled to work toward allied objectives and lead his force to its ultimate destruction.

Based on the premise that information is a strategic asset, a portion of IW doctrine seeks to disrupt or deny access to information in order to seize initiative from an adversary. The other half of IW doctrine seeks to maintain the integrity of our information gathering and distribution infrastructure.[4]

Applying Information Warfare

Most modern political and military C^2 systems are based on high speed communications and computers. It follows that this information infrastructure, also known as an "infosphere", will be the arena in which information warfare is waged. Any system or person who participates in the C^2 process will be a potential target in an IW campaign.

An excellent example of an early IW campaign can be seen in the conduct of OPERATION DESERT STORM. In order to gain air supremacy, a joint special operations aviation force opened a breach in radar coverage surrounding Iraq. The Iraqi command was unaware the breach existed until a blow had been struck from which Iraq would never recover. Simultaneously, a coordinated attack by stealth aircraft against Iraq's air defense headquarters bunker and three regional air defense centers effectively turned Iraq's integrated air defense network into a hodgepodge of uncoordinated air defense fiefdoms, each of which could be neutralized independently at the coalition forces' leisure. No longer did a surface-to-air missile site have a regional C^2 system to prioritize and provide early warning of approaching targets. Later in the campaign, a baited hook was thrown to news agencies when reporters--desperate for a story--were allowed to cover exercises in preparation for an amphibious assault into Kuwait. This successful psychological operation by a Marine Amphibious Brigade and Navy special forces held five Iraqi divisions in place on the east coast while two corps of coalition forces shifted to the western flank for the final assault.

In a similar way, an IW campaign will focus against the enemy infosphere. It will be necessary to isolate, identify and analyze each element of an enemy infosphere in order to determine portions which can affect the OODA loop's size. Once these areas of the enemy infosphere are identified, an attack against critical nodes would deny access to information, destroy the information, or render it useless to the adversary forces. Even more damaging, information warriors could alter data in a network, causing the adversary to use false information in his decision making process and follow a game plan of the friendly commander's design.

A significant portion of emerging IW theory attempts to grasp the impact of employing computer technology as a weapon system. Computer programs could take on the roles of etherial spies and warriors as they seek to impede an enemy's access to reliable information, while allowing friendly forces to form a reliable picture of enemy intentions and actions. While operational security and electronic warfare protect the integrity of our C^2 systems, "software strikes" could be conducted against critical C^2 nodes and data. Computer hardware could complement other weapon systems to deliver strikes against the enemy command and control system.

Information warfare can affect political, economic or military targets. A televised news conference with an important dignitary could be altered to change its content. IW could sabotage an economy by reducing international confidence in a nation's currency, or causing an adversary to default on payments. Access to critical research and development facilities could be interfered with. Satellite communications could be terminated. Strategic information warfare waged independently could cause an adversary to lose faith in his own data management systems, greatly increasing confusion and difficulty of controlling assets. On an operational level, interference with enemy data management systems could create damaging time delays in the enemy's ability to make and implement decisions. On the tactical level, IW would be able to compliment the use of other systems to reduce danger to friendly forces and increase chances for success.

Information warfare opens new avenues for the conduct of politico-military operations. On the low level of the conflict spectrum, covert intrusion into an opponent's command and control system may provide unique insight into their political intentions and decision making process. As tensions rise, it may be necessary to send a signal to demonstrate our concern. In the science fiction movie classic *The Day the Earth Stood Still*, an alien named Klaatu immobilized the Earth for an hour to demonstrate his power. While the United States may not be able to halt all activity, shutting down a telephone system or financial network for an hour may have the desired effect. If it becomes necessary to conduct full-scale intervention, IW can compliment other military forces by gathering intelligence, subverting and denying enemy communications or even destroying information networks.

Since information warfare theory is grounded in the appearance of new information systems technology, it may be useful to examine the emergence of other new technologies throughout history. This may provide valuable lessons learned for the modern day military theorist. Advocates of air-to-air missiles declared the demise of gun armed fighter aircraft in the late 1950s. Military officers who were developing intercontinental ballistic missiles touted the end of manned strategic bombers. In some circles, the advent of submarines in World War I sounded a siren's song for surface warships. Anti-tank missiles employed in the 1973 Arab-Israeli war were hailed as ending the tank's dominance on the battlefield. In all of these cases, new technologies ultimately complimented existing technologies in warfare; they did not render the old ways obsolete. On the other hand, artillery replaced the catapult and archer. Horses and beasts of burden were replaced by mechanization. Naval aviation did push the battleship into obsolescence. There will certainly be those who argue that information warfare renders other forms of warfare obsolete. Tactics and

operational art will no doubt change to accommodate IW doctrine. Some of these changes may be quite unprecedented. In all likelihood, though, IW will serve to compliment existing technology rather than push it into obsolescence. Whether IW will be a mere evolutionary development or a revolutionary one remains to be seen.

IW takes advantage of technological opportunities as novel to today's military theorist as the tank was to Churchill, Fuller and Guderian in the early part of our century. IW is an area as ripe for contemplation and experimentation as the concept of strategic bombardment was to Douhet and Mitchell. Although an information warrior won't be able to demonstrate the effectiveness of IW with the same flair Billy Mitchell used to demonstrate the capabilities of independent air power, a coordinated software assault could cripple strategic targets in an enemy nation's infrastructure. Indeed, IW is a concept which merits serious research by the twenty-first century warrior.

We should not examine the merits of IW without examining its shortcomings. First and foremost, the potential impact of IW is directly proportional to the sophistication of one's adversary. The craftiest computer program will be useless against an enemy who communicates by beating on logs with sticks. Indeed, the Vietnam War and recent UN experience in Somalia illustrate how a determined, well-led force can overcome a technologically advanced opponent. The utility of IW increases in direct proportion to the adversary's reliance on information systems. Therefore, while information warfare systems will be an effective addition to our national arsenal, we must avoid considering IW a panacea for conducting engagements across the conflict spectrum.

Fighting the Information War

Every time we pick up a magazine, turn on the television or listen to the radio, it seems we hear a new story about computers. A small flaw discovered in the Pentium microprocessor, causes a decline in Intel stock.[5] A scare results from to an erroneous warning sent out on the INTERNET about an alleged "Good Times" computer virus. Microsoft markets computer software products to China.[6] A popular movie plot centers around computer hackers who steal an experimental decryption device which provides access to traffic on any computer network.[7] Computers, information networks and similar command and control (C2) systems have made remarkable strides, having a significant impact on nearly every business and government activity in the United States.

One development with implications for the military is the appearance of "hackers" and "phreakers"--persons who gain unauthorized access to computer and telephone systems, respectively. Since their emergence in the 1970s, hackers have repeatedly demonstrated their talent at overcoming computer security systems to access information. In some cases, intruders have gone beyond merely accessing a system; malicious damage has been done to computer databases, causing millions of dollars in loss to corporations and agencies. In most cases, hackers are amateur sleuths who simply treat secure computer systems as the world's greatest puzzle. But what if hacking were done for a more subtle, deliberate purpose? What if an organization of hackers

cooperated in a coordinated attempt to gain access to a computer system? What if careful planning and preparation allowed this access to be gained with no trace left behind in the violated C2 system?

Implications of hacking and phreaking for intelligence collection are simple to grasp. A computer network or telephone system is designed to transmit information. Much of that information will form an excellent intelligence picture of an adversary. Simply monitoring the quantity of information flowing through a network can serve as an indicator of pending activity. Readers who served in the military may remember how the Department of Defense's TEMPEST program taught us all that the emissions from electronic equipment can be picked up from remote distances. The TEMPEST program taught us to take precautions against unauthorized monitoring. Computer networks can be monitored through telephone modems, peripheral equipment, power lines, human agents and other means. The information contained in these systems can be monitored without the user's knowledge.

Take this idea one step further. If a system can be monitored remotely, it might also be accessed remotely. A program could be installed to record and relay computer access codes to a remote location. In a simple brute force approach, hardware could be destroyed or an electromagnetic pulse sent through the system to render it inoperative. Logic bombs inserted into a system could neutralize a vital program on command. Even more subtle efforts could be made--imagine the implications of a simple program which adds one degree of altitude and azimuth to the firing solutions computed by every targeting radar in an enemy air defense network. The enemy might never know the computer intrusion occurred until every shot missed and the antiaircraft site was destroyed.

Information and access to information have become a strategic asset whose destruction or denial has a profound effect on military operations and national security. The 1989 stock market crash was assessed to be a result of computer trading activity run amok. Imagine the impact on the United States if Wall Street were held hostage by a computer virus which threatened to destroy financial records. Ponder the effect on military operations if all phone lines for a US unified command were suddenly rerouted to the local pizza delivery shop. Contemplate the impact on morale if a military unit's pay records suddenly disappeared. If a critical presentation for a new business account were "misplaced" on the day of an important meeting, it could mean a great loss for a major corporation and great gain for a competitor. Losing access to data at a critical time could spell the difference between success and failure on the international playing field.

Employing computers as a weapon system will introduce a new glossary of terminology for the information warrior. Computer warfighting weapons can be divided into four categories: software, hardware, electromagnetic systems and other assets.

Software consists of programs designed to collect information on, inhibit, alter, deny use of, or destroy the enemy infosphere. Software would be the primary soldier in pure information

warfare. One example of a software asset--called a KNOWBOT--could serve as a virtual software spy. Other examples of software warfighting assets have exotic, computer hacker names: "demons", "sniffers", "viruses", "Trojan horses", "worms" or "logic bombs".[8] A more detailed description of these "weapon systems" may help the reader visualize more effectively the potential use of software assets in IW.

- **KNOWBOT**. The Corporation for National Research Initiatives has coined the term KNOWBOT, or knowledge robot. A KNOWBOT is "a program which moves from machine to machine, possibly cloning itself. KNOWBOTs can communicate with one another, with various servers in a network, and with users. They could be dispatched to do our bidding in a global landscape of computing and information resources".[9] The intelligence implications of using a KNOWBOT as a "software spy" are self evident. A KNOWBOT could be introduced into enemy computer systems, reproducing itself when it detects information meeting desired specifications. The KNOWBOT clone would then collect information and report when interrogated, at a predetermined time, or feed a continuous stream of information to intelligence users. The KNOWBOT could even be programmed to relocate or erase itself to prevent discovery of espionage activity. Finally, KNOWBOTs could seek out, alter or destroy critical nodes of an enemy C^2 system.

- **Demon**. A program which, when introduced into a system, records all commands entered into the system. When retrieved and interrogated, the demon reports all commands used on the computer system for a given time period. Demons can reveal access codes, encryption keys or similar information for systems.[10] Similar to the demon is the "**sniffer**". A sniffer records the first 128 bits of data on a given program. Logon information and passwords are usually contained in this portion of any data stream. Because they merely read and record data, such programs are very difficult to detect.

- **Virus**. A program which, upon introduction, attaches itself to resident files or tables on a machine or network. The virus spreads itself to other files as it comes into contact with them. It may reproduce without doing any actual damage, or it may erase files via the file allocation table.[11]

- **Trap Door**. A back door into a system, written in by a programmer to bypass future security codes. Trap doors provide quick entry to a system if the programmer needs to make changes at a later date. The risk of a trap door occurs when the wrong person finds it; unauthorized access to the system is made easy and security systems are circumvented.[12]

- **Trojan Horse**. A code which remains hidden within a computer system or network until it emerges to perform a desired function. A Trojan Horse can authorize access to the system, alter, deny or destroy data, or slow down system function.[13]

- **Worm**. A nuisance file which grows within an information storage system. It can alter files, take up memory space, or displace and overwrite valuable information.[14]

- **Logic Bomb**. This instruction remains dormant until a pre-determined condition occurs. Logic bombs are usually undetectable before they are activated. When the pre-determined condition occurs, the program activates. The logic bomb can alter, deny or destroy data and inhibit system function.[15] The pre-determined condition may be a certain time, a command initiated by the computer user, or a command sent from outside the C^2 system. Thus, logic bombs could be installed into enemy C^2 nets during heightened national tension, and activated if hostilities commence.

Hardware. The primary purpose of a hardware asset is to bring software assets into contact with an enemy computer system. Hardware primarily consists of computers and peripheral components. Any piece of equipment connected to a computer, be it a fiberoptic or telephone cable, facsimile machine or printer, is capable of transmitting information to that computer. Therefore it is a potential avenue for gaining access to the infosphere. During Operation DESERT STORM, *US News & World Report* magazine cast light on an attempt to introduce a virus into an Iraqi computer system. The writers stated that a virus was programmed into a chip, surreptitiously placed into a computer printer.[16] This is an excellent example of a hardware asset used to introduce a software strike into the enemy infosphere. The information infrastructure itself also falls into the hardware category, since software assets can gain access to hardware by being introduced via the enemy information network.

Electromagnetic Systems. Any mechanisms using the electromagnetic spectrum to subvert, disrupt or destroy enemy command and control are electromagnetic systems. This essentially includes any system capable of Meaconing, Intrusion, Jamming and Interference (MIJI). Meaconing interferes with direction finding and navigation. Intrusion confuses enemy communications by broadcasting counter-commands or walking over communications. Jamming and interference prevents the enemy from using a portion of the electromagnetic spectrum. Recent Department of Defense research into disabling systems offers yet another option. Conventional explosives can now produce a massive, focused electromagnetic pulse (EMP). These weapons were reportedly used against Iraq in the Gulf War.[17] Unprotected electronic circuitry will be overloaded if it is within the lethal envelope of an EMP event. EMP simply shorts-out electronic equipment.[18]

Other Assets. This catch-all category makes an important point. Information warfare is not limited to electronic systems. A laser-guided bomb dropped onto a cable junction box can have a very direct and significant effect on the enemy infosphere. Downing power or telephone lines can disable a command post. Special forces can destroy critical nodes or capture key personnel associated with the IW function. A motorized infantry division can overrun a critical node in a communications network. Simply put, non-computer assets can compliment use of computer hardware and software assets, or can act unilaterally. Their goal is to achieve the desired effect upon the enemy C^2 network in pursuit of strategic, operational or tactical objectives.

In the hands of a skilled team of information warriors, these technical assets described above can operate independently, or compliment other assets in pursuit of national goals. Successful employment of IW assets could theoretically end a war before the first shot is fired.

Controlling the Information War

Controlling an information war will be a challenge to conventional military structure. A simple keystroke by a low-level "cyberwarrior" could have serious national policy ramifications if it affects an adversarial strategic system. For example, denying an adversary the use of national intelligence systems at a critical time could escalate a tense confrontation to a nuclear exchange. Such strategic action would have to be taken only with Presidential consent. Other action would be less serious, and could be controlled at a lower level. Therefore, IW could be waged on multiple levels--tactical, operational and strategic. Potential targets cross military, economic or political lines. Control of IW systems must be vested in an authority competent to weigh myriad factors involved in a decision to employ such capability.

An information warfare campaign will span organizational and service boundaries to compliment other systems in the pursuit of strategic objectives. A war planner trying to orchestrate an IW campaign would no doubt benefit from thorough research into the development of joint and combined war plans with similar scope. Air Tasking Orders, the Single Integrated Operations Plan (SIOP), artillery fire plans and tasking procedures for national intelligence collection systems may provide an understanding of the coordination and planning necessary to conduct a successful IW campaign. Control procedures and decision making processes used in managing national military and intelligence assets will certainly provide pertinent source material to those attempting to formulate integrated IW campaign plans. Thoroughly planned IW will be a powerful asset for all branches of the military, national intelligence agencies and national leadership.

A successful IW campaign requires intimate coordination between command, communications, operations, logistics and intelligence disciplines. In an IW campaign, the lines of distinction between the traditional military functions would blur, and the disciplines eventually merge. Computer networks and means of information exchange have dramatically altered the face of the business world. In many cases, traditional "stovepipe" command and control structures will impede rapid information transfer. Many businesses find it necessary to cut middle level management, reducing the impediments between those with the authority to decide what should to be done and those who know how to do it. Such restructuring results in a flat, weblike organization known in some circles as a "blueberry pancake". Organizational structure will certainly evolve in order to take advantage of new capabilities and implement new doctrine. The traditional disciplines described above may indeed meld into a cohesive organization or task force directed at critical nodes of an enemy's ability to make and implement decisions.

When assigning budgetary and operational responsibility for IW, national policy makers must select a lead agency with a good track record controlling programs with multiple-interest implications. The Air Force would certainly be a contender to serve as this lead agency. The USAF has demonstrated a superb capability to carry out such activities through its airlift, joint and combined air operations and space programs. The USAF is also the service most capable to handle advanced technology and new, innovative systems such as stealth, precision-guided munitions, integrated airspace management systems and battlefield management systems. With its high proportion of college graduates, the USAF will be able to provide the proper personnel to control such a capability for the United States. United States Special Operations Command (USSOCOM) may also be a good host for IW. IW is, by its very nature, unconventional warfare. It spans the spectrum of conflict in the same manner as do special operations. IW, like special operations, affects a broad range of targets with far-reaching impact. Psychological operations--considered a major component of IW--have been traditionally conducted by special operations forces. Finally, USSOCOM is familiar with operations conducted both in support of theater commanders and in response to Presidential directives.

Legal Considerations for Information Warfare Doctrine

Our legal system is struggling to keep pace with the rapid expansion of available information systems technology. The accessibility of information has raised fundamental constitutional issues for government officials and legal scholars. Computer hackers are at odds with security representatives from corporate and government organizations. The recent controversy regarding the US government-sponsored "Clipper Chip" highlighted the government's concern over the spread of computer encryption technology and the ability of national agencies to monitor international and domestic information exchange.[19] International law is even more vague regarding information technology. International agreements regulate use of proprietary information, communications and international commerce; but belligerent use of information systems technology remains unaddressed.

In its most basic form, a legal code for information warfare will probably take the form of a simple quid pro quo agreement; i.e., if someone does it to us, we feel absolutely free to do it to them. Legal precedent exists for this practice in the Hague Conventions. In these documents, "a number of nations, including the United States, issued a reservation stating that first use by a belligerent of chemical and biological weapons authorized the state subject to the attack to respond in kind...."[20] The US used these reservations as justification to develop and maintain a chemical and biological warfare capability. The United States therefore has legal precedent in developing an IW capability. The United States has a vested interest in preserving "freedom of the infosphere," very much in the same way we currently exercise freedom of navigation. The threat of IW may even evolve along similar lines to that of the threat presented by anti-ballistic missiles and nuclear weapons. If this happens, nations may ultimately be compelled to conclude agreements similar to

"Open Skies", in which all nations agree to allow limited access into their computer networks and C^2 systems in order to foster mutual trust. Information warfare may even pose such a threat to a nation's welfare that it will negotiate treaties to limit or ban information warfare altogether.

This leads us to a fundamental moral question. Should the United States develop an information warfare capability? There are compelling reasons to do so.

- Other nations are already committing computer espionage against the United States. Those nations may also be formulating plans to exploit our C^2 networks and undermine our defense capability. The bestseller *The Cuckoo's Egg* described a recent computer espionage attempt. Unknown computer hackers in Europe were able to obtain information and documents over a computer network stretching thousands of miles. Our allies are no exception--experts have identified France, Germany, Japan, Israel and Taiwan among at least 20 foreign intelligence agencies conducting computer espionage against US businesses.[21] At present, approximately $200 billion per year is lost to industrial espionage.[22] It is apparent that computer-based intelligence collection and IW activity would have to take place within international convention during peacetime, or significant political embarrassment could arise as a result of a poorly planned operation.

- The US lacks doctrine for conducting information war. Our national security policy and warfighting doctrine do not address computers as a tool capable of carrying out independent offensive or defensive operations. In addition, the rapid advances in computer technology make keeping up with that technology a full time job. The sooner we begin planning a coherent information warfare doctrine, the more secure our nation will be. It is gratifying that top military leaders are beginning to formulate a cohesive national security C^2 attack and defense policy.[23] Such action is a good first step in developing IW doctrine.

- Computers and C^2 systems had little commonality before the 1990s. The military services especially have lacked compatible C^2 systems and software. Major efforts are underway to correct these problems.[24] But if all military services use common or compatible information systems, then all services will be equally vulnerable to actions against those systems. Future information systems must be able to withstand a coordinated assault from any avenue of approach, yet provide friendly forces with critical information rapidly and accurately. This capability must be designed into systems as they are in the conceptual phase of development, rather than scabbed on as an afterthought. The systems being designed today are the systems with which our nation will conduct IW tomorrow.

- National security policy does not yet acknowledge the absolutely critical role computers and information systems play in military operations. Information networks are a high-value asset that warrant protection. One recent estimate placed the value of US information management systems at ten percent of our gross national product.[25] Loss of these systems would, by definition, decimate our nation's economy. A study conducted by *Information Week* magazine revealed chief

executives in American businesses "continue to downplay data security issues, even as the threats rise."[26] If similar opinions exist in the national security community as well, then there is cause for concern. US governmental information security policy lags far behind the capabilities of modern information transfer systems. Security measures must be incorporated into information systems as they're designed.

Popular thought on information warfare raises another legal issue. At what point will monitoring of and intrusion into another country's C^2 network constitute a violation of international convention? At some point--probably when a government takes action to deny access to, alter or destroy data--a line will be crossed between prudent intelligence collection and hostile intent. National decision makers must determine at what point intrusion into another government's infosphere will indicate hostile intent or constitute an act of war. This decision will also serve notice regarding the point at which the United States would perceive IW hostilities to commence, warranting US response. Damage to US information systems will legally permit the US to conduct punitive software strikes in retaliation for that damage. National policy makers must determine the potential degree of damage, and plan how the United States will respond to such an event.

IW opens up a political and moral can of worms for national leadership as well. Alvin and Heidi Toffler recently coined the term "Anti-War"[27] to describe the concept of rendering enemy equipment ineffective before it could be used in battle. The United States has conducted considerable research into this field.[28] This may make it possible to minimize loss of life to the adversary. However, an enemy who does not possess the technology to engage in IW may have to resort to the less advanced, brutal methods--often described by Army Rangers as "killing people and breaking things." IW may make it unnecessary for US forces to exact a proportionate loss of life on an enemy. A potential political consequence of IW for friendly forces may be a greater loss of life on the friendly side than on the enemy side. This possibility has tremendous implications for American political leadership. General Colin Powell described the plan of military operation against Iraq very succinctly; "First we're going to cut it off, then we're going to kill it." But when the coalition achieved its stated goals, President Bush was able to call a halt to the ground attack in Operation DESERT STORM before it was necessary to destroy the Iraqi ground forces. This decision has been debated since the war's end. In the near future, political leaders may find an angry American public demanding "payback time" when such an effort is unnecessary. The question for a political leader is simple. Once you cut it off, *should* you kill it? This no-win scenario would be a terrible moral dilemma for any democratically elected leader.

These are but a few of the legal and moral issues raised by IW theory. Although information itself will not cost lives, denial or subversion of that information may lead to lives lost. It will be important to tomorrow's US military officer that a clear understanding of the legal issues for IW be reached. Rules of engagement must be established prior to conducting an IW campaign. If these limitations are not established by national command authorities, law of the jungle will reign supreme in the conduct of IW.

Conclusion

IW doctrine has significant implications for modern military theory. Under IW, the enemy soldier no longer constitutes a major target. IW will focus on preventing the enemy soldier from talking to his commander. Without coordinated action, an enemy force becomes an unwieldy mob, and a battle devolves to a crowd-control issue. In the not too distant future, computer weapon systems will conduct "software strikes" against the enemy infosphere to disrupt command and control. Targets will be chosen for military, political or economic significance. IW opens new doors throughout the spectrum of conflict to achieve tactical, operational and strategic objectives.

Information warfare is a concept which is only now beginning to make its way through governmental and military circles. The technology currently exists with which to conduct an IW campaign. National leaders must reflect on the implications of this new technology in order to develop coherent policy and rules of engagement. Many legal questions remain unaddressed. Intelligence agencies will have to evaluate the benefit of coordinated "hacking" and "phreaking" to obtain critical intelligence information while maintaining plausible denial of US involvement. Military professionals will have to consider IW's impact on operations. They must plan how best to deliver strikes against an enemy command and control infrastructure and to preserve the integrity of their own infosphere. IW will no doubt become the subject of Capitol Hill budgetary battles as agencies vie to determine which will be top IW dog.

Much more study and discussion must take place before information warfare theory evolves into practical doctrine for planning an IW campaign. IW may either be a revolutionary development, or merely an evolutionary one. What is certain is that IW promises to dramatically impact the way we fight. Individual or group research, thought and discussion of information warfare will benefit those planning for military service in the twenty-first century.

SOURCES:

BOOKS:

David Baker; *The Shape of Wars to Come*; New York; Stein and Day, Publishers; 1982.

Bruce G. Blair; *Strategic Command and Control*; Washington, D.C.; The Brookings Institution; 1985.

Alan D. Campen, ed; *The First Information War*; Fairfax, VA; AFCEA International Press; 1992.

Dr Ray S. Cline; *Intelligence Warfare: Today's Advanced Technology Conflict*; New York; Crescent Books; 1983.

Mario de Arcangelis; *Electronic Warfare from the Battle of Tsushima to the Falklands and Lebanon Conflicts*; Poole, Dorset; Blandford Press; 1985.

John Keegan; *The Mask of Command*; New York; Viking Penguin Inc; 1987.

RobertLeonhard; *The Art of Maneuver: Maneuver Warfare and AirLand Battle*; Novato, CA; Presidio Press; 1991.

W. Michael Reisman and Chris T. Antoniou; *The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict*; New York; Vintage Books (Random House); 1994.

Winn Schwartau, *Information Warfare - Chaos on the Electronic Superhighway*; New York; Thunder's Mouth Press; 1994.

Richard Simpkin; *Race to the Swift: Thoughts on 21st Century Warfare*; London; Brassey's Defense Publishers; 1985.

BruceSterling; *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*; New York; Bantam Books; 1992.

US News & World Report, ed; *Triumph Without Victory*; New York; US News & World Report; 1991.

Alvin and Heidi Toffler; *War and Anti-War: Survival at the Dawn of the 21st Century*; Boston; Little, Brown and Company; 1993

Timothy N Trainor and Diane Krasnewich; *Computers! (Second Edition)*; Santa Cruz, CA; Mitchell Publishing, Inc; 1989.

Jay Tuck; *The T Directorate: How the KGB Smuggles NATO's Strategic Secrets to Moscow*; New York; St Martin's Press; 1986.

Bruce W. Watson, Bruce George, Peter Tsouras, B.L. Cyr; *Military Lessons of the Gulf War*; London, Greenhill Books; 1991.

Bob Woodward; *The Commanders*; New York; Simon & Schuster; 1991.

PERIODICALS:

"Army Prepares for Non-Lethal Combat"; *Aviation Week and Space Technology*; Washington DC; May 24, 1993; 62

TSgt Ray Baker; "BUG!"; *Spokesman, the Official Newsletter for the USAF Electronic Security Command*; Nov 91.

Maj Jason B. Barlow, USAF; "Strategic Paralysis: An Air Power Strategy for the Present"; *Airpower Journal*, Vol VII, No 4 (Winter 1993); Maxwell AFB AL; Air University; 4

William J. Broad; "Doing Science on a Network: A Long Way From Gutenberg"; *The New York Times*; New York; May 18 1993; C1

Thomas Y. Canby and Charles O'Rear; "Advanced Materials - Reshaping our Lives"; *National Geographic Magazine*, Vol 176, No 6 (Dec 89); Washington DC; The National Geographic Society; 746

John B. Carnett; "The Digital Warrior"; *Popular Science*, Vol 245, no 3 (Sep 94); New York; Popular Science; 60

"Computers: Chip Shot"; *US News & World Report*, Vol 117, No 23; 12 Dec 94.

Roland Dannreuther; *Adelphi Papers 264--The Gulf Conflict: A Political and Strategic Analysis*; London; Brasseys/International Institute for Strategic Studies; Winter 1991/92.

Bob Davis; "The Clipper Chip is Your Friend, NSA Contends; *The Wall Street Journal*; 22 Mar 94

Lt Col Allan W. Debban, USAF; "Disabling Systems: War-Fighting Option for the Future"; Airpower Journal, Vol VII, No 1 (Spring 1993); Maxwell AFB AL; Air University; 44.

Phillip Elmer-DeWitt; "Who Should Keep the Keys?"; *Time*; 14 Mar 94

David A. Fulghum; "EMP Weapons Lead the Race for Non-Lethal Technology"; *Aviation Week & Space Technology*; Washington DC; May 4, 1993; 61

"Future Soldier Advances on Multiple Fronts"; *International Defense Review*, Vol 27 (12/94); Soulsdon, Surrey UK; Janes Information Group; 24

Barton Gellman; "Revisiting the Gulf War"; *The Washington Post*; Washington DC; July 25, 1993; A20

Vincent P. Grimes; "Army Building Digital Foundation for the Future - Electronically Connecting Combat Units Promises Dramatic Increase in Punch"; *National Defense* Vol LXXIX, No 503 (Dec 94); Arlington VA; American Defense Preparedness Association; 16

Vincent P. Grimes; "Army Begins Digitization Buildup"; *International Defense Review*, Vol 27 (7/94); Soulsdon, Surrey UK; Janes Information Group; 57

Mark Hewish; "Fishing in the Data Stream - Netting Information is the Trick"; *International Defense Review*, Vol 27 (7/94); Soulsdon, Surrey UK; Janes Information Group; 51

Maj Roger C Hunter, USAF; "Disabling Systems and the Air Force"; *Air Power Journal*, Vol VIII, No 3 (Fall 1994); Maxwell AFB AL; Air University; 43

Phillip J. Klass, ed; Special Report on Electronic Warfare, *Aviation Week and Space Technology*; Washington DC; Oct 19, 1992; 36-82

Maj David Nicholls, USAF and Maj Todor D. Tagarav, Bulgarian Air Force; "What Does Chaos Theory Mean for Warfare?"; *Air Power Journal*, Vol VIII, No 3 (Fall 1994); Maxwell AFB AL; Air University; 48

John G. Roos; "InfoTech InfoPower"; *Armed Forces Journal International* (June 1994); Washington DC; AFJI; 31

Jeffrey I. Schiller; "Secure Distributed Computing"; *Scientific American*, Vol 271, No 5 (Nov 1994); New York; Scientific American, Inc; 72

John Schwartz and John Mintz; "Chipping Away at a Fundamental Freedom?"; *The Washington Post*; 2 Mar 94.

John Schwartz; "The Security 'Threat' to Your Software--US Fears Foreign Use of Common Encryption Features"; *The Washington Post*; 18 Jun 94.

William B. Scott; "War Breaker Intelligence & Planning Project Aims to Cut Strike Cycle Times"; *Aviation Week and Space Technology*; Washington DC; Jun 7, 1993; 151

William B. Scott; "War Breaker Program Explores New Sensor, Targeting Systems"; *Aviation Week and Space Technology*; Washington DC; May 31, 1993; 37

Barbera Starr; "Pentagon Maps Non-Lethal Technologies"; *International Defense Review*, Vol 27 (7/94); Soulsdon, Surrey UK; Janes Information Group; 30

Gowrishankar Sundaram, ed. "Defense Electronics and Computing, No 1" *International Defense Review*, Editorial Supplement to Feb 1990 Issue; Soulsdon, Surrey UK; Janes Information Group

Gowrishankar Sundaram, ed. "Defense Electronics and Computing, No 2" *International Defense Review*, Editorial Supplement to Apr 1990 Issue; Soulsdon, Surrey UK; Janes Information Group

Vic Sussman; "Decoding the Electronic Future: Will Encryption Secure or Deny Privacy Rights?"; *US News & World Report*; 14 Mar 94.

Various; "Communications, Computers and Networks--How to Work, Play and Thrive in Cyberspace"; *Scientific American Special Issue*, Volume 265, Number 3; New York; Scientific American, Inc; September 1991.

Vilino, Bob and Joseph C. Panettieri; "Tempting Fate"; *Information Week*, Issue 445; CMP Publications, Inc; Manhasset NY; 6 Oct 93

Paul Wallich; "Trends in Communication - Wire Pirates"; *Scientific American*, Vol 270, No 3 (March 1994); New York; Scientific American, Inc; 90

Steve R. White, David M. Chess and Chengi Jimmy Kuo; *Coping with Computer Viruses and Related Problems*; Sept 21, 1989; Milford CT; Copyright IBM Corporation 1989

Samuel B. Griffith, *Sun Tzu - The Art of War,* Oxford University Press, New York, 1963, p 77.

Gary Horne and Nancy LeBruin (producers); "hack attack"; The Discovery Channel (in association with Yorkshire Television); Dece

.

he "OODA Loop" has been used to illustrate command decision making cycles by many military theorists. This author first became aware o l through a fellow officer, who heard a speech by the commander of Air Intelligence Agency, Major General Minihan. Lieutenant General Minih Assistant Chief of Staff, USAF Intelligence.

recently ordered and received Winn Schwartau's incisive book, *Information Warfare.* On initial glance, the book addresses many of the same i ssed by this paper. Although it does not address application of IW from a military perspective and is not extremely detailed, the book offers intere rios and is a useful reference.

Computers: Chip Shot"; *US NEWS AND WORLD REPORT,* Vol 117, No 23; December 12th 1994.

All Things Considered"; *National Public Radio*; 8 Dec 1994.

SNEAKERS, starring Robert Redford and Sydney Poitier, 1993.

TSgt Ray Baker; "BUG!", *SPOKESMAN, the official newsletter for the USAF Electronic Security Command;* November 1991.

Vinton G Cerf.; "Networks"; *SCIENTIFIC AMERICAN*, Special Issue; September 1991.

TSgt Ray Baker; "BUG!", *SPOKESMAN, the official newsletter for the USAF Electronic Security Command*; November 1991.

Ibid

Ibid

Ibid

Ibid

Ibid

US News and World Report, Ed.; *Triumph Without Victory*; US News and World Report; 1991. Schwartau's *Information Warfare* ma incing case that this incident was possibly a hoax or a misinterpreted event. To the best of my knowledge, no official confirmation or denial o ent has been made by the US government. True or not, the report serves to illustrate the potential use of hardware to convey a software assault.

Barton Gellman; "Revisiting the Gulf War"; *The Washington Post*; Washington DC; July 25, 1993; A20. To the best of my knowledge, th rnment has not officially commented on this article.

David A. Fulghum; "EMP Weapons Lead Race for Non-Lethal Technology"; *Aviation Week & Space Technology*; Washington DC; May 24, 19

Vic Sussman; "Decoding the Electronic Future"; *US News & World Report;* March 14th 1994.

W. Michael Reisman and Chris T. Antoniou, ed.; *The Laws Of War*; Vintage Books; New York; 1994; p. 58

Gary Horne and Nancy LeBruin (producers); "hack attack"; *The Discovery Channel* (in association with Yorkshire Television); December 1994.

Bob Vilino and Joseph C. Panettieri; "Tempting Fate"; *Information Week*, Issue 445, CMP Publications, Inc; Manhasset NY; 6 Oct 93; p 48.

I was recently told that several documents have been identified as the foundation for US military thought on information warfare. These are DO .1, *Information Warfare*; CJCS MOP 30, *Command and Control Warfare*; and JCS Publication 3-13, *Command and Control Warfare Operati* rtunately, these documents have not yet become available at my level.

Vincent P. Grimes; "Army Building Digital Foundation for Future - Electronically Connecting Combat Units Promises Dramatic Increase in Pu *nal Defense*, Vol LXXIX, No 503 (Dec 94); Arlington VA; American Defense Preparedness Association; 16.

lso Vincent P. Grimes; "Army Begins Digitization Buildup"; *International Defense Review*, Vol 27 (7/94); Soulsdon, Surrey UK; Jane's Inform p; 57.

lso Mark Hewish; "Fishing in the Data Stream - Netting Information is the Trick"; *International Defense Review*, Vol 27 (7/94); Soulsdon, Surrey Information Group; 51.

lso John G. Roos; "InfoTech InfoPower"; *Armed Forces Journal International* (June 94); Washington DC; AFJI; 31.

"Computers and Information Networks"; *SCIENTIFIC AMERICAN*, Special Issue; Sep 91.

Bob Vilino and Joseph C. Panettieri, "Tempting Fate", *Information Week,* Issue 445, CMP Publications, Inc, Manhasset, NY, 6 Oct 93, pp 42-52.

Alvin and Heidi Toffler; *War and Anti-War,* Survival at the Dawn of the 21st Century; New York NY; Little, Brown and Company; 1993

Lt Col Alan W Debban, USAF; "Disabling Systems: War-Fighting Option for the Future"; *Airpower Journal*, Vol VII, No 1 (Spring 1993); Ma AL; Air University; 44.

lso Barbera Starr; "Pentagon Maps Non-Lethal Technologies"; *International Defense Review*, Vol 27 (7/94); Soulsdon, Surrey UK; Janes Inform p; 30.